INTRODUCTION TO 21 CFR PART 11, ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

1

Part 11 Subparts

A - General

B - Electronic Records

C - Electronic Signatures

2

§ 11.2 Implementation

- Submissions records - need
  - Part 11 compliance;
  - Record in Docket 92S-0251

3

Electronic Record

"any combination of text, graphics, data, audio, pictorial, or other information representation in *digital form* that is created, modified, maintained, archived, retrieved, or distributed by a *computer system*."

4

§ 11.3 Definitions

- **Electronic signature**

"a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the *legally binding equivalent* of the individual's handwritten signature."

5

§ 11.3 Definitions

- **Handwritten signature**

"the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form."

Continued ...

6

§ 11.3 Definitions

- **Handwritten signature**

"The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark."

7

§ 11.3 Definitions

- **Digital signature**

"an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified."

8

§ 11.3 Definitions

- **Biometrics**

"a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable."

9

§ 11.3 Definitions

- **Closed system**

"an environment in which system *access is controlled* by persons who are *responsible* for the *content* of electronic *records* that are on the system."

10

§ 11.3 Definitions

- **Open system**

"an environment in which system *access is not controlled* by persons who are *responsible* for the *content* of electronic *records* that are on the system."

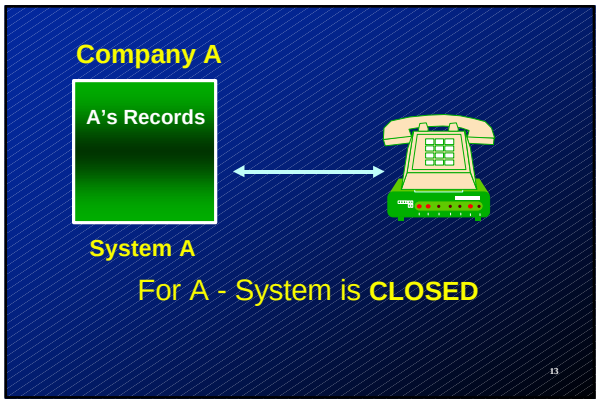
11

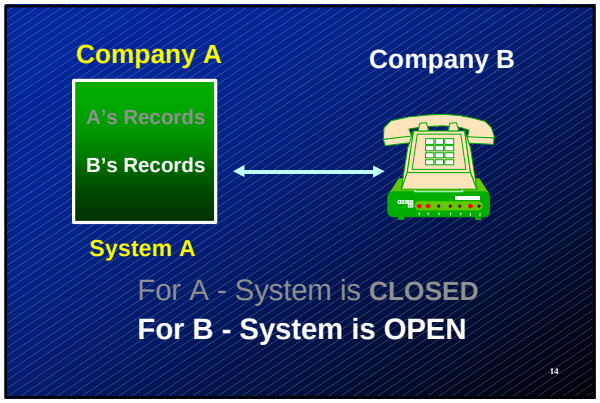
Company A

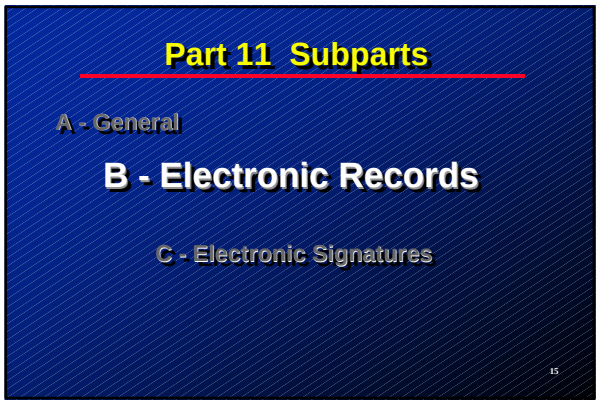
System A

For A - System is **CLOSED**

12


Company A
A's Records
System A
For A - System is CLOSED
13


Company A
Company B
A's Records
B's Records
System A
For A - System is CLOSED
For B - System is OPEN
14


Part 11 Subparts
A - General
B - Electronic Records
C - Electronic Signatures
15

§ 11.10 Controls for closed systems

- Controls designed to ensure:
  - Authenticity
  - Integrity
  - Confidentiality (as appropriate)
  - Against signer ready repudiation

16

§ 11.10 Controls for closed systems

- Validation, to ensure
  - Accuracy/reliability
  - Consistent intended performance
  - Discern invalid/altered records

17

§ 11.10 Controls for closed systems

- Ability to make copies that are:
  - Accurate and complete
  - Human readable and electronic
    - Suitable for FDA review/copying

18

§ 11.10 Controls for closed systems

- Archiving:
  - Accurate/ready retrieval throughout retention period
- System access limitation
  - Only authorized individuals

19

§ 11.10 Controls for closed systems

- Audit trails that are:
  - Secure
  - Operator independent
  - Computer generated
  - Time-stamped (date & time)

20

§ 11.10 Controls for closed systems

- Audit trails must cover:
  - Operator entries/actions that cause e-record
    - Creation
    - Modification
    - Deletion

21

§ 11.10 Controls for closed systems

- Audit trail documentation:
  - Retain per base e-record
  - Available for FDA review/copying
- Record changes not to obscure prior info

22

§ 11.10 Controls for closed systems

- Operational system checks, as appropriate to:
  - Enforce step/event sequencing

23

§ 11.10 Controls for closed systems

- Authority checks on individuals
  - System use
  - Signing
  - Operational access/performance
  - Input/output device access

24

§ 11.10 Controls for closed systems

- Device checks, as appropriate
  - Validity of source
    - Operational instruction
    - Data input

25

§ 11.10 Controls for closed systems

- Personnel qualifications
  - Education, training & experience
  - People who develop, maintain, or use
    - E-record/e-sig systems

26

§ 11.10 Controls for closed systems

- Accountability policies
  - Written & followed
  - Hold people accountable/responsible for actions under e-sigs
    - Deter record/signature falsification

27

§ 11.10 Controls for closed systems

- Control systems documentation
  - Operation/maintenance docs.
    - Distribution, access & use
  - Change control
    - Audit trail of modifications

28

§ 11.30 Controls for open systems

- Designed to ensure e-record:
  - Authenticity
  - Integrity
  - Confidentiality, as appropriate
- From creation to receipt

29

§ 11.30 Controls for open systems

- Include §11.10 controls, as appropriate:
- Added measures, per circumstances, to ensure:
  - Authenticity, Integrity
  - Confidentiality, as appropriate

more...

30

§ 11.30 Controls for open systems

- Examples of added measures:
  - Document encryption
  - Digital signatures

31

§ 11.50 Signature manifestations

- Info associated w/E-record must clearly show:
  - Signer's printed name
  - Date/time of signing
  - Meaning of signature
    - E.g., review, approval

32

§ 11.50 Signature manifestations

- Signature info:
  - Subject to e-record controls
  - Part of e-record human readable form
    - Electronic display
    - Printout

33

§ 11.70 Signature/record linking

- Link to ensure sigs can't be:
  - Excised
  - Copied
  - Otherwise transferred
- Prevent e-record falsification by *ordinary means*

34

Part 11 Subparts

A - General

B - Electronic Records

C - Electronic Signatures

35

§ 11.100 General Requirements (E-Sigs)

- Unique to one individual
  - No reuse by someone else
  - No reassignment

36

§ 11.100 General Requirements (E-Sigs)

- Verify individual ID before e-sig (or e-sig element) is:
  - Established
  - Assigned
  - Certified
  - Otherwise sanctioned

37

§ 11.100 General Requirements (E-Sigs)

- Certification to FDA:
  - What - Intent
    - E-sigs = H-sigs, legally binding
  - When - Pronto
    - Before, or at time of, e-sig use
      - First, but Not each use

38

§ 11.100 General Requirements (E-Sigs)

- Certification to FDA:
  - How - Paper letter
    - Over h-sig
  - Where - FDA HQ
    - Office of Regional Operations
      - HFC-100, Rockville, MD 20857

39

§ 11.100 General Requirements (E-Sigs)

- Certification to FDA:
  - Scope - Global:
    - One per enterprise
  - More - Per FDA request re. specific e-sig:
    - Certification or testimony

40

Pursuant to §11.100 of Title 21 of the Code of Federal Regulations, this is to certify that {organization name} intends that all electronic signatures executed by our employees, agents, or representatives, located anywhere in the world, are the legally binding equivalent of traditional handwritten signatures.

41

§ 11.200 E-sig components and controls

- Non-biometric e-sig:
  - Two distinct components:
    - E.g., User ID and password

42

§ 11.200 E-sig components and controls

- Non-biometric e-sig:
  - Multi-signings, one continuous controlled access:
    - 1st signing: all components
    - 2nd+ signing: ≥ 1 component:
      - designed for signer's use only
      - executable by signer only

43

§ 11.200 E-sig components and controls

- Non-biometric e-sig:
  - Multi-signings NOT in one continuous controlled access:
    - each signing: all components

44

§ 11.200 E-sig components and controls

- Non-biometric e-sig:
  - Used only by genuine owners
  - Attempted use by others (Part 11 doesn't sanction such use.)
    - Multilateral collaboration needed

45

§ 11.200 E-sig components and controls

- Biometric e-sig:
  - Designed to ensure use only by genuine owners

46

§ 11.300 Controls for id codes/passwords

- Persons must use controls to ensure security & integrity
- Unique ID/PW combo:
  - No 2 people have same ID/PW

47

§ 11.300 Controls for id codes/passwords

- Periodically check, recall, or revise issuance
  - E.g., address pw aging

48

§ 11.300 Controls for id codes/passwords

- Loss management procedures
  - Deauthorize potentially compromised devices that:
    - Bear/generate id/pw info
  - Issue replacements
    - Use suitable, rigorous controls

49

§ 11.300 Controls for id codes/passwords

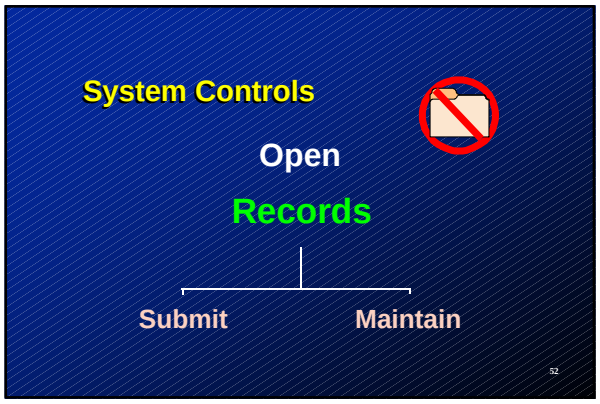
- Unauthorized use safeguards
  - Report attempts in *urgent* & *immediate* manner to:
    - Security unit
    - Management, as appropriate

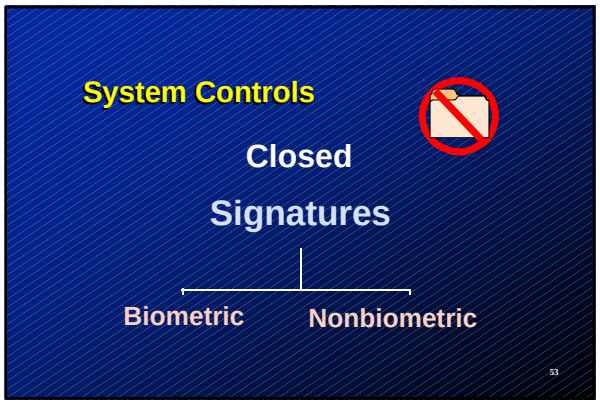
50

§ 11.300 Controls for id codes/passwords

- Initial & periodic device testing
  - Things that bear/generate
    - Id/pw info
  - Test for:
    - Proper functioning
    - Unauthorized alterations

51





Part 11 Enforcement Warning Letters & 483s

- Some have issued
- CGMP warning letters w/part 11 issues
  - Clear w/HQ
    - Re: part 11 aspect only
    - Temporary measure

54

Part 11 Enforcement CPG 7153.17

- Legacy systems (in use before 8/20/97)
  - Not exempt from rule
  - Technical controls may take longer to implement
  - Expect immediate steps toward compliance

55

Part 11 Enforcement CPG 7153.17

- Reg actions (case by case)
  - Nature/extent of deviation
  - Effect on product quality/data integrity
  - Adequacy/timeliness of corrective action plan
  - Compliance history

56

Part 11 Enforcement CPG 7153.17

- Reg action HQ consults
- Pending firm's full compliance:
  - Increased FDA vigilance; e.g.,
    - Inconsistencies
    - Unauthorized changes
    - Poor attribution

57

Part 11 Enforcement CPG 7153.17

- Worst case
  - Predicate rule violated
  - Tie deviation to predicate rule

58

Resources

- Internet :
  - http://www.fda.gov/cder/esig/part11.htm
  - http://www.fda.gov/dockets
- Intranet (Part 11 Certifications)
  - http://www.ora.fda.gov:8000/ora/deio/esig.html

59

Resources

- Guidance for Industry:
  - Computerized Systems Used In Clinical Trials
- Guidance for FDA
  - ORA's Investigations Operation Manual
    - Part 11 Answers to FAQs

60